PCT/EP 99 / 10405

Europäisches Patentamt
4

European Patent Office

Office européen des brevets

EPO - DG 1

04. 02. 2000

EP99/10405

(74)

Bescheinigung Certificate Attestation

REC'D 15 FEB 2000
WIPO PCT

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

09/623643

Patentanmeldung Nr. Patent application No. Demande de brevet n°

99100168.6

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

I.L.C. HATTEN-HECKMAN

DEN HAAG, DEN
THE HAGUE,
LA HAYE, LE 14/01/00

EPA/EPO/OEB Form 1014 - 02.91

This Page Blank (uspto)

Europäisches Patentamt | European Patent Office | Office européen des brevets

Blatt 2 der Bescheinigung
Sheet 2 of the certificate
Page 2 de l'attestation

Anmeldung Nr.: / Application no.: / Demande n°: 99100168.6

Anmeldetag: / Date of filing: / Date de dépôt: 07/01/99

Anmelder: / Applicant(s): / Demandeur(s):
Philips Corporate Intellectual Property GmbH
52064 Aachen
GERMANY

Bezeichnung der Erfindung: / Title of the invention: / Titre de l'invention:
Constant current supply regulator for Smartcard Ics

In Anspruch genommene Priorität(en) / Priority(ies) claimed / Priorité(s) revendiquée(s)

Staat: / State: / Pays:	Tag: / Date: / Date:	Aktenzeichen: / File no. / Numéro de dépôt:

Internationale Patentklassifikation: / International Patent classification: / Classification internationale des brevets:
/

Am Anmeldetag benannte Vertragstaaten: / Contracting states designated at date of filing: / Etats contractants désignés lors du depôt:
AT/BE/CH/CY/DE/DK/ES/FI/FR/GB/GR/IE/IT/LI/LU/MC/NL/PT/SE

Bemerkungen: / Remarks: / Remarques:
The applicant's name at the time of filing was as follows :
Philips Patentverwaltung GmbH

Philips Patentverwaltung GmbH
Koninklijke Philips Electronics N. V. PHD 99-001 EP-P

Description

Constant Current Supply Regulator for Smartcard Ics

Summary

A circuit for contactless smart cards based on the following two subcircuits.

1) A supply source with the following two characteristics:
- at the receiving side the load is independent on the load at the delivering side;
- at the delivering side, the source behaves over a wide range as a current source.

Such a supply source can be constructed using a shunt-type power regulator.

2) An information processing circuit that operates over a wide range of the supply voltage by adapting its speed.

Such processing circuits can be constructed using self-timed (asynchronous) circuits.

The combination of the two subcircuits (1) and (2) offers the following advantages:

- No interference of processing circuit with the communication;

- Protection against ‚Differential Power Analysis' (DPA) techniques (even the EM radiation does not contain any information, since the current in the total circuit only depends on the power received);

- Maximum performance for the power received;

- Smaller supply capacitor for filtering required.

Detailed Description

Smart Card ICs usually contain an embedded supply voltage regulator. The function of this block can be adapting of internal to external voltage levels and/or stabilisation of the internal supply voltage.

The circuitry in the Smart Card like a micro-processor and an encryptor/decryptor unit doesn't draw a constant supply current. The currently used supply concept doesn't have a good suppression to these fluctuations. In case of contactless Smart Cards a large internal capacitor is needed in order to prevent interference with the Modulation for backward communication. Even worse is the fact that the supply current is data dependent. It seems that this data dependency can be measured externally, which would give an opportunity to break Smart Card protection codes. This analysis technique is called DPA.

The present idea is to prevent these problems by making the external supply current independent of the internal fluctuations. A constant current is delivered to the Smart Card IC, which is either used for operation of the circuit or dumped via a shunt current path so that the internal supply voltage stays within certain margins. Peak load of the circuitry are averaged in time by a buffer capacitor at the internal supply. **Figs. 1a** and **1b** show this concept. Essential is that current source function is not part of a speed limited control loop depending on output variables, which ensures a constant current independent of load activity. The shunt block has a limiting function which prevents that the current source is pinched off if the load circuitry doesn't consume all the delivered power. It's also used to limit the internal supply voltage to a certain absolute maximum value (which is the usual regulator function). The 'constant' current value of the regulator may depend on the external input voltage and can therefore be adapted to the voltage-power relation of the load circuitry. **Figs. 2 and 3** show possible implementations of this idea.

Additional measures can be taken, especially avoiding a generation of code-dependent supply currents or making supply currents less predictable.

Advantage / Improvements:

This supply concept is especially interesting in combination with asynchronous logic, because supply voltage, power and speed are automatically tracking with each other in this case so large variations of the internal supply are possible and a minimum amount of buffer capacitance is needed.

Application / Use:

Security of Smart Cards against "Differential Power Analysis".

Brief Description of the Drawings

Fig. 1a shows a basic circuit diagram of a first embodiment of the invention,

Fig. 1b shows a basic circuit diagram of a second embodiment of the invention,

Fig. 2 shows a first implementation of the invention,

Fig. 3 shows a second implementation of the invention,

Fig. 4 shows a basic circuit diagram of a Smart Card Power Supply Architecture for contacted and non-contact (contactless) Smart Cards,

Fig. 5 shows a basic circuit diagram of the so-called 'Differential Power Analysis',

Fig. 6 shows a basic circuit diagram of an improved architecture of contacted and non-contact (contactless) Smart Cards, making use of the present invention.

Claims

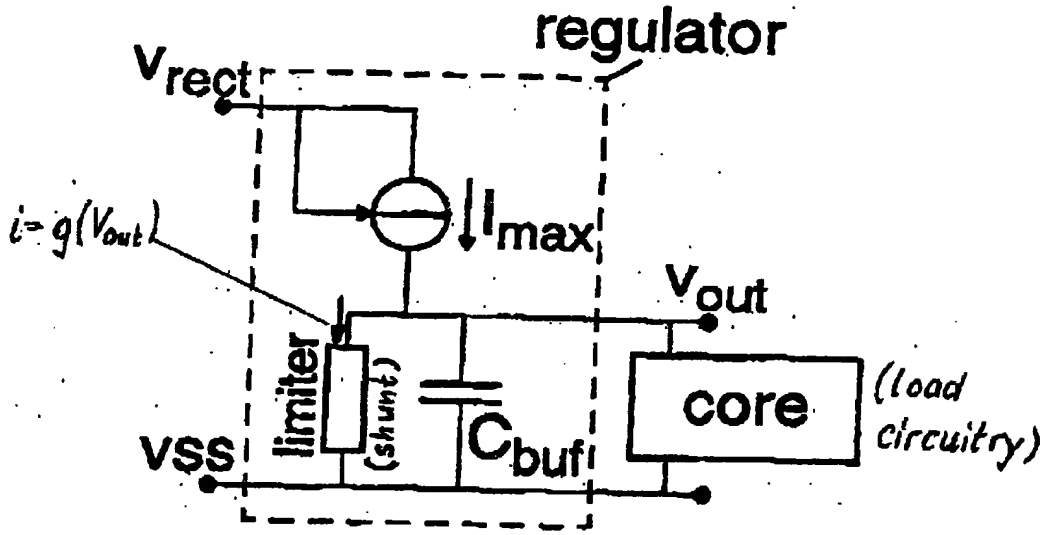
1) A supply source, characterised in that
- at the receiving side the load is independent on the load at the delivering side;
- at the delivering side, the source behaves over a wide range as a current source.

2) A supply source as claimed in claim 1, characterised in being constructed using a shunt-type power regulator.

3) A supply source as claimed in claim 1, characterised in an information processing circuit that operates over a wide range of the supply voltage by adapting its speed.

4) A supply source as claimed in claim 3, characterised in that the information processing circuit is constructed using self-timed (asynchronous) circuits.

Proposed Regulator Structure



- I_{max} 'only' depends on V_{rect}, but can be adaptable
- Limiter:
  - a) drains unused power,
  - b) regulates V_{out}
  - c) safeguard operation of current source
- C_{buf} performs time averaging on power peaks

Fig. 1a

PHD 99-001 EP-P

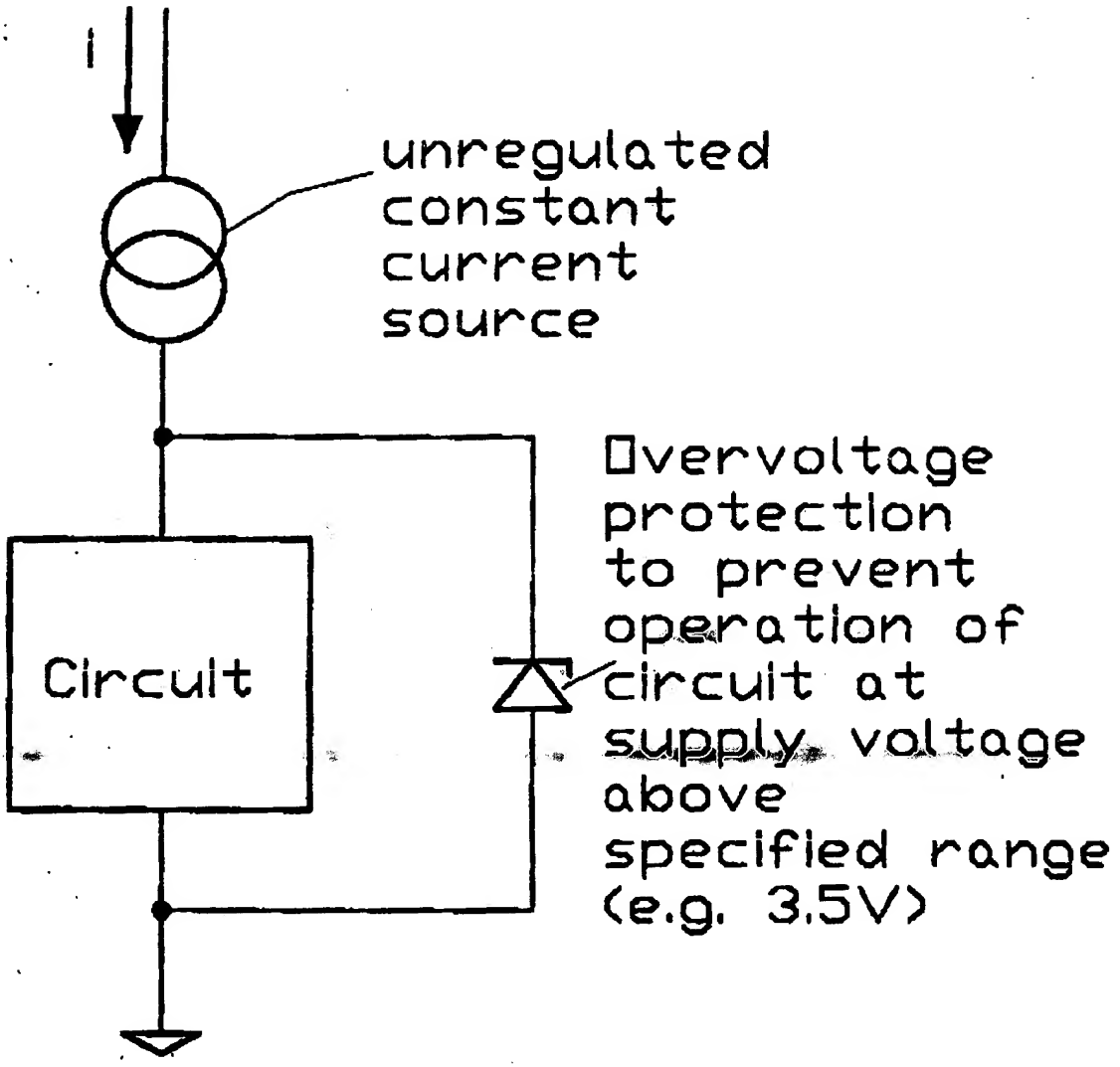


Fig. 1b

PHD 99-001 EP-P

PHD 99-004EP-D

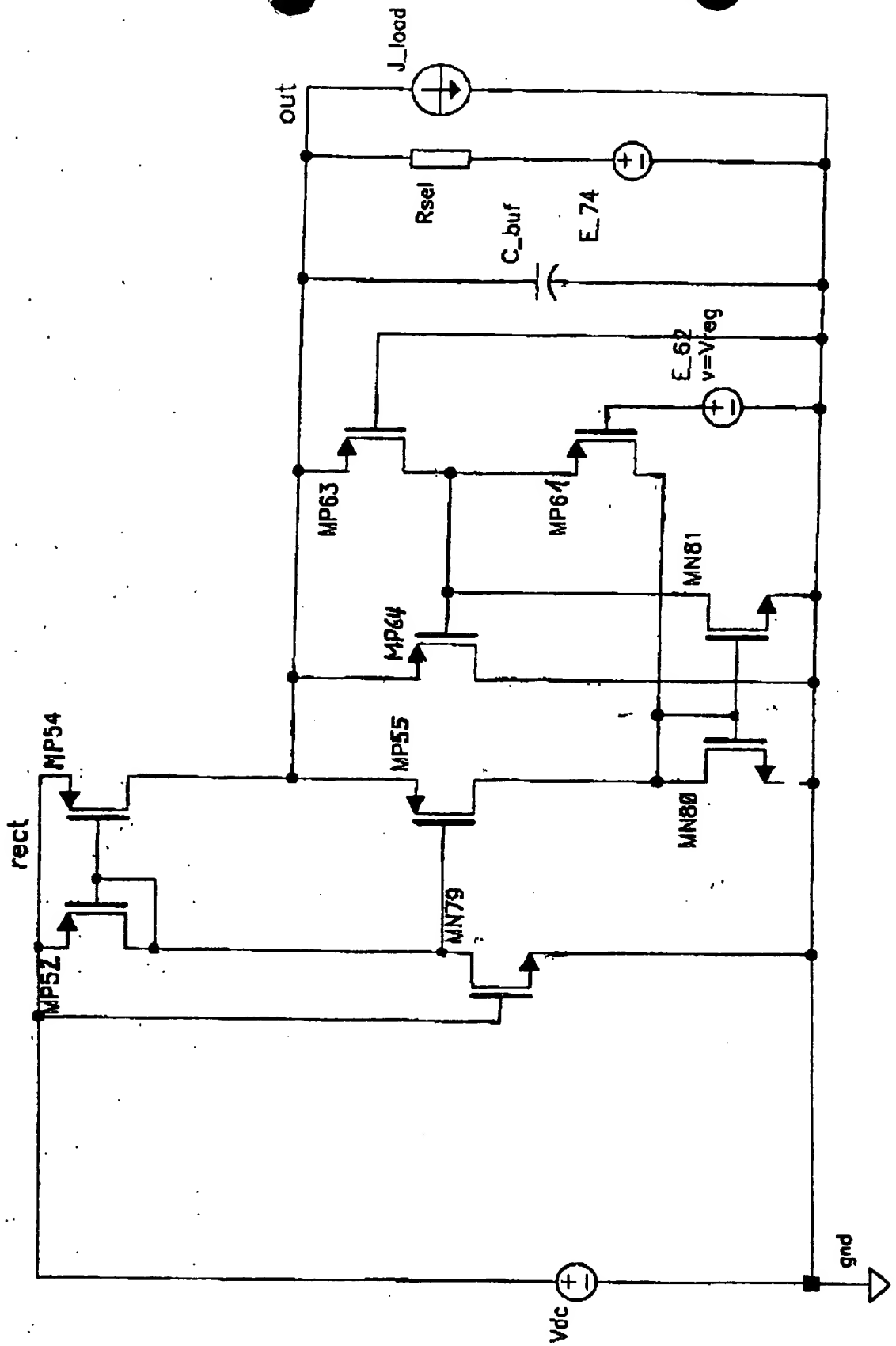


Fig. 2

PHD 98-041EP-P

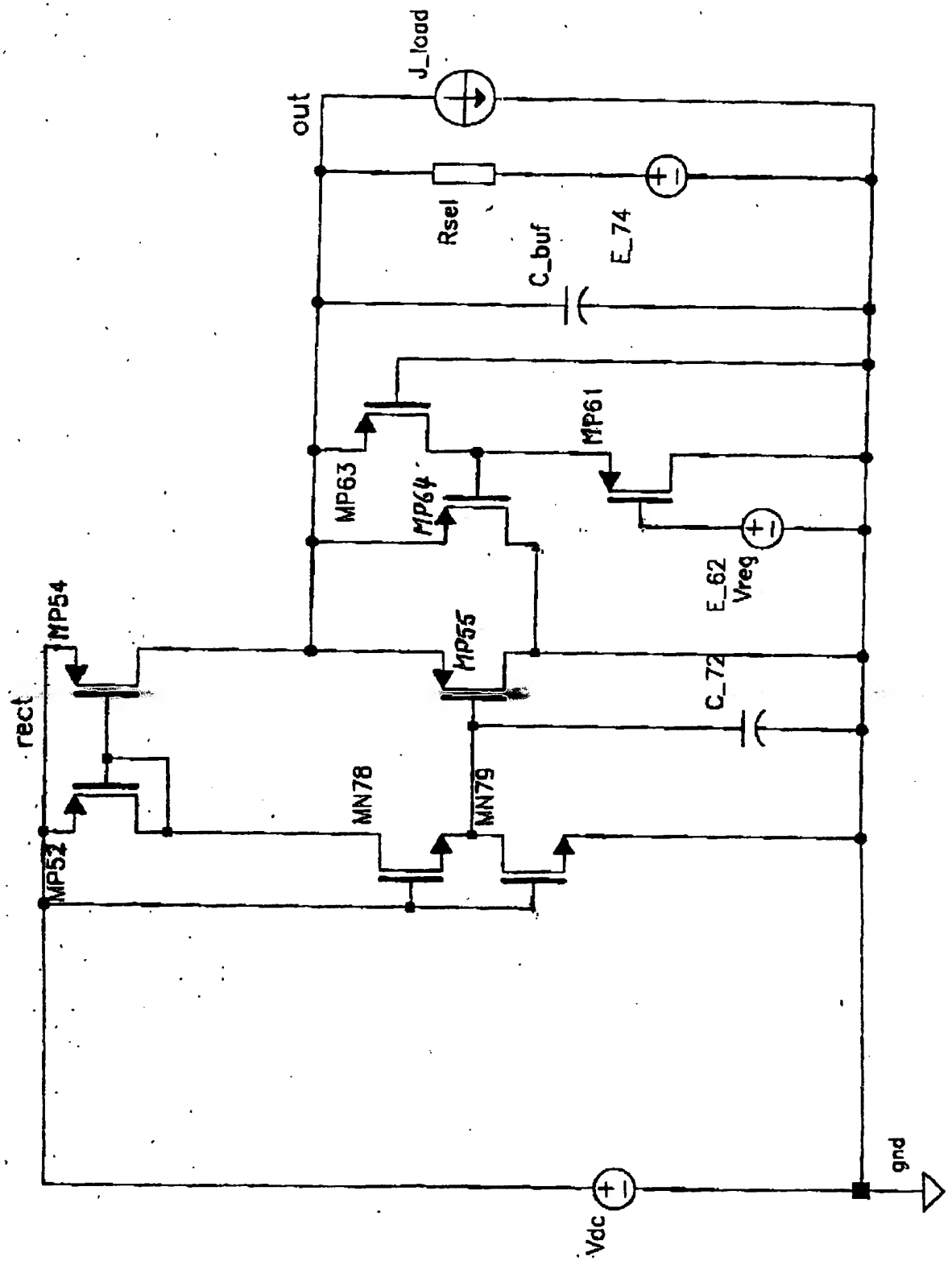
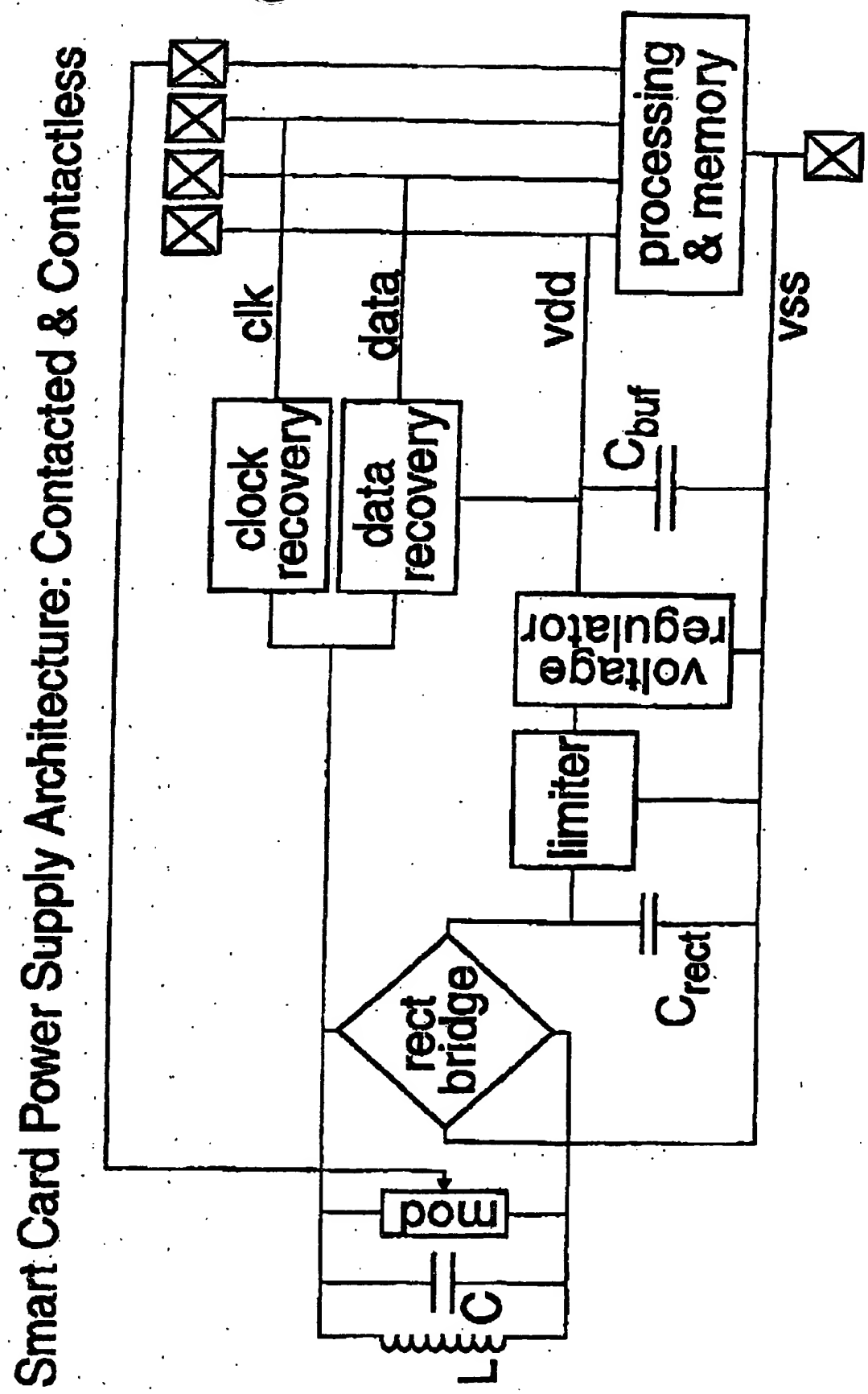


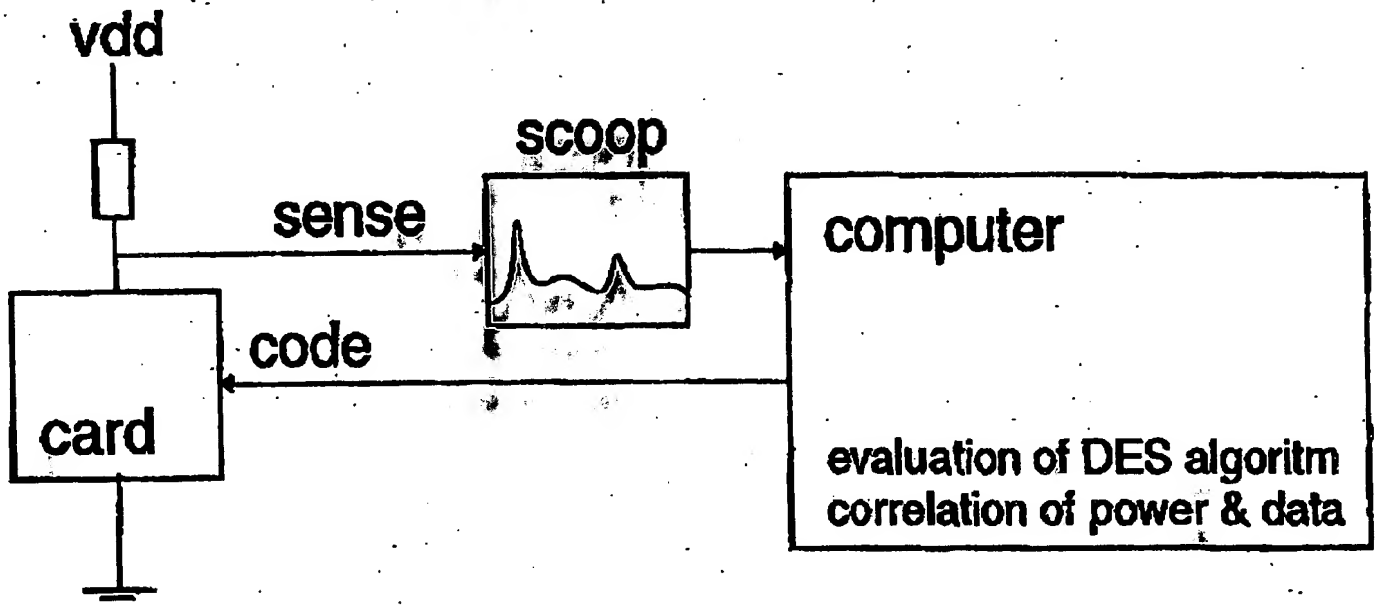
Fig 3



PHD 99-004EP-D

Fig. 4

DPA: Differential Power Analysis



- Recent method to crack the cards security code (triple DES)
- Detect correlation between supply current behaviour and codes

--> Target = decrease code dependency of supply current!

Fig. 5

PHD 99-001 EP-P

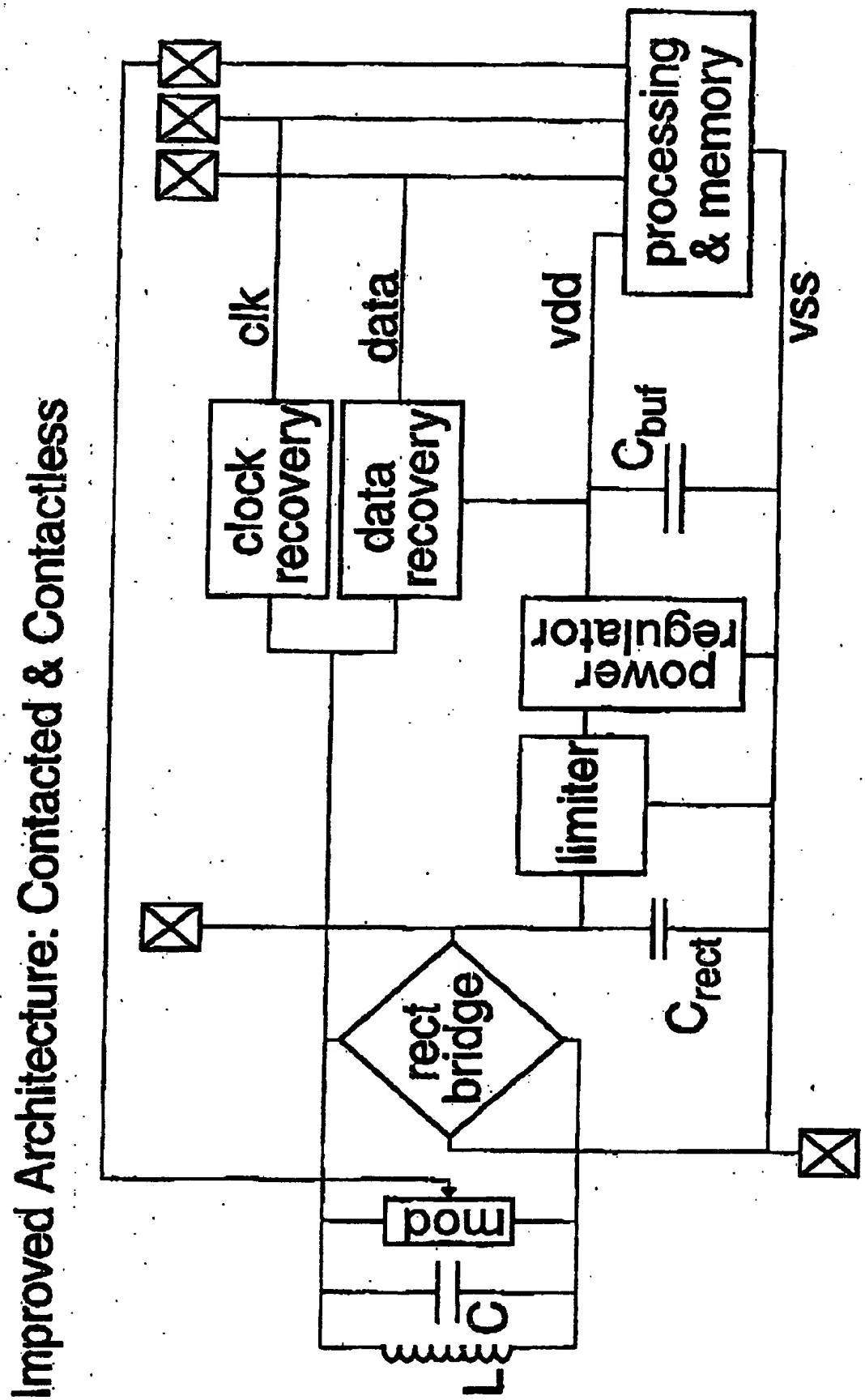


Fig. 6

PHD 99-004 EP-P

Abstract

A circuit for contactless smart cards based on the following two subcircuits.

1) A supply source with the following two characteristics:
- at the receiving side the load is independent on the load at the delivering side;
- at the delivering side, the source behaves over a wide range as a current source.

Such a supply source can be constructed using a shunt-type power regulator.

2) An information processing circuit that operates over a wide range of the supply voltage by adapting its speed.

Such processing circuits can be constructed using self-timed (asynchronous) circuits.

Advantage / Improvements:

The combination of the two subcircuits (1) and (2) offers the following advantages:

- No interference of processing circuit with the communication;
- Protection against ‚Differential Power Analysis' (DPA) techniques (even the EM radiation does not contain any information, since the current in the total circuit only depends on the power received);
- Maximum performance for the power received;
- Smaller supply capacitor for filtering required.

Application / Use:

Smart Cards